

2005 REPORT TO THE PRESIDENT



INFORMATION
SECURITY
OVERSIGHT
OFFICE

AUTHORITY

Executive Order 12958, as amended, "Classified National Security Information," and Executive Order 12829, as amended, "National Industrial Security Program." The Information Security Oversight Office (ISOO) is a component of the National Archives and Records Administration (NARA) and receives its policy and program guidance from the National Security Council (NSC).

MISSION

ISOO oversees the security classification programs in both Government and industry and reports annually to the President on their status.

FUNCTIONS

- Develops implementing directives and instructions.
- Maintains liaison with agency counterparts and conducts on-site reviews and special document reviews to monitor agency compliance.
- Develops and disseminates security education materials for Government and industry; monitors security education and training programs.
- Receives and takes action on complaints, appeals, and suggestions.
- Collects and analyzes relevant statistical data and, along with other information, reports them annually to the President.
- Serves as spokesperson to Congress, the media, special interest groups, professional organizations, and the public.
- Conducts special studies on identified or potential problem areas and develops remedial approaches for program improvement.
- Recommends policy changes to the President through the NSC.
- Provides program and administrative support for the Interagency Security Classification Appeals Panel (ISCAP).
- Provides program and administrative support for the Public Interest Declassification Board (PIDB).
- Reviews requests for original classification authority from agencies.
- Chairs interagency meetings to discuss matters pertaining to both Executive orders.
- Reviews and approves agency implementing regulations and agency guides for systematic declassification review.

GOALS

- Promotes and enhances the system that protects the national security information that safeguards the American Government and its people.
- Provides for an informed American public by ensuring that the minimum information necessary to the interest of national security is classified and that information is declassified as soon as it no longer requires protection.
- Promotes and enhances concepts that facilitate the sharing of information in the fulfillment of mission-critical functions related to national security.
- Provides expert advice and guidance pertinent to the principles of information security.

INFORMATION SECURITY OVERSIGHT OFFICE

May 25, 2006

The President
The White House
Washington, DC 20500



Dear Mr. President:

We are pleased to submit to you the 2005 Report of the Information Security Oversight Office (ISOO).

This report provides information on the status of the security classification program as required by Executive Order 12958, as amended, "Classified National Security Information."

It includes statistics and analysis concerning components of the system, primarily classification, declassification, and the ISOO review program. It also contains information with respect to industrial security in the private sector as required by Executive Order 12829, as amended, "National Industrial Security Program" (NISP).

One of the most notable developments is that the Public Interest Declassification Board is now holding regular sessions. This Board will contribute to the declassification process by identifying records on specific subjects that are of extraordinary public interest. These records will be identified when it is deemed that declassification will not undermine the national security interests of the United States.

ISOO also finalized the coordination of an implementing directive for Executive Order 12829, as amended, NISP. The directive will provide additional guidance to agencies concerning NISP management.

In addition, ISOO continued to focus on evaluating Executive branch progress toward the orderly declassification of classified records of permanent historical value that are 25-years-old or older. For the most part, the Executive branch is progressing well toward the deadline of December 31, 2006, although challenges for full implementation by December 31, 2009, remain.

A responsible security classification system and a committed declassification program are the cornerstones of an open and efficient government that serves to protect and inform its citizens. Ensuring that these cornerstones are properly placed requires diligence and integrity with regard to the American ideals of providing for our national security within the context of a free and open society.

Respectfully,

J. William Leonard
Director

SUMMARY OF FISCAL YEAR 2005 PROGRAM ACTIVITY

The following Report to the President is the 10th report under Executive Order 12958, which went into effect in October 1995 and was most recently amended on March 25, 2003. The following data highlight agency reporting and Information Security Oversight Office (ISOO) analysis.

CLASSIFICATION ACTIVITY

- Executive branch agencies reported 3,959 original classification authorities.
- Agencies reported 258,633 original classification decisions.
- Executive branch agencies reported 13,948,140 derivative classification decisions.
- Agencies reported 14,206,773 combined classification decisions.

DECLASSIFICATION ACTIVITY

- Under Automatic and Systematic Review Declassification programs, agencies declassified 29,540,603 pages of historically valuable records.
- Agencies received 3,517 new mandatory review requests.
- Under mandatory review, agencies declassified in full 66,569 pages; declassified in part 70,743 pages; and retained classification in full of 13,348 pages.
- Agencies received 152 new mandatory review appeals.
- On appeal, agencies declassified in whole or in part 2,720 additional pages.

TABLE OF CONTENTS

Letter to the President	1
Summary of Fiscal Year 2005 Program Activity	2
A Better Way	3
Interagency Security Classification Appeals Panel	4
National Industrial Security Program	8
Classification	9
Declassification	14
MDR Special Review	22
Public Interest Declassification Board	25
Reviews	26
Agency Acronyms and Abbreviations	inside back cover

A BETTER WAY

This past year marked the 10th anniversary of Executive Order (E.O.) 12958, as amended, “Classified National Security Information.” One of the most significant advances of this groundbreaking framework was the introduction of the automatic declassification concept. This model calls for all 25-year-old and older records of permanent historical value containing classified national security information to be declassified, exempted, excluded, referred to other interested agencies, or appropriately delayed before attaining their 25-year-old status. It is one thing to conceive such a concept and quite another to implement it. Nonetheless, on December 31, 2006, after several delays, the concept of automatic declassification will finally be implemented, at least for those agency records that do not contain classified information originated by or of interest to another agency.

For the most part, the Executive branch is progressing toward fulfilling its responsibilities for records of permanent historical value containing classified information by the initial deadline of December 31, 2006; however, it is doing so by utilizing a largely agency-centric approach. While such a method has positioned most agencies to successfully fulfill their individual responsibilities under the automatic declassification process, it is inadequate in standing up to the challenge of handling records that contain information of interest to multiple agencies. Recent attention focused on the withdrawal of previously declassified records from the open shelves of the National Archives exemplifies some of the shortcomings of the current approach. We clearly have to find a better way. It is certain that complete implementation of automatic declassification by December 31, 2009, can only succeed on an Executive branch-wide basis.

KEY ELEMENTS OF A BETTER WAY INCLUDE THE FOLLOWING:

- Develop an Executive branch-wide approach to declassification of records that better integrates individual agency efforts, produces more reliable results, and is more efficient in process.
- Enhance agency understanding of each other’s sensitive information.
- Provide additional training that develops the needed understanding.
- Establish centralized databases and other resources to facilitate sound declassification decisions.
- Provide for greater consistency in the level of review applied to records.
- Preclude redundancies in security reviews.
- Increase the interface between declassification reviews done under the Executive order and those for other requests for access to information, such as the Freedom of Information Act (FOIA).
- Establish centralized priorities.
- Achieve greater rationalization of resources.
- Improve oversight.

In response to these challenges, it is essential that a new way of doing business be established that has the authority, expertise, and resources to ensure that the decisions to either declassify or continue the classification of Federal government records of permanent historical value are appropriate and reflect the best informed judgments of all parties. There are a number of examples in which a concerted Executive branch-wide approach has worked in the past two decades, such as the Iran-Contra, Prisoners of War/Missing in Action (POW/MIA), Chile-Pinochet, and Nazi War Crimes special reviews.

Furthermore, more needs to be done to develop standardized guidelines and protocols, facilitating better understanding of the various dynamics entailed in assessing and determining the appropriate action to take following a declassification review, and ensuring greater consistency in results. More than anything else, we need to streamline the multiple, inefficient, and, at times, ineffective independent agency reviews of the same material. Finally, we must also ensure that declassified records are made available for public research as soon as possible, consistent with governing laws and regulations. We must implement a better way if agencies are to fully implement the groundbreaking framework created more than 10 years ago.

INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

AUTHORITY

Section 5.3 of E.O. 12958, as amended, “Classified National Security Information.”

The Intelligence Reform Act of 2004 established the Office of the Director of National Intelligence (ODNI) and amended the National Security Act of 1947 to strike the Director of Central Intelligence (DCI) from the pertinent portions. The responsibilities and the authorities of the DNI and the Director of the Central Intelligence Agency (DCIA) with regard to decisions of the Interagency Security Classification Appeals Panel (ISCAP) are currently being addressed. As a result, the declassification by the ISCAP of certain information previously owned or controlled by the DCI is pending.

FUNCTIONS

- Decides on appeals by authorized persons who have filed classification challenges under section 1.8 of E.O. 12958, as amended.
- Approves, denies, or amends agency exemptions from automatic declassification as provided in section 3.3 of E.O. 12958, as amended.
- Decides on appeals by persons or entities who have filed requests for Mandatory Declassification Review (MDR) under section 3.5 of E.O. 12958, as amended.

MEMBERS

The following members were in the specified positions as of the end of FY 2005:

William H. Leary, Chair
National Security Council

James A. Baker
Department of Justice

Edmund Cohen
Central Intelligence Agency

Margaret P. Grafeld
Department of State

Carol A. Haave
Department of Defense

Michael J. Kurtz
National Archives and Records Administration

EXECUTIVE SECRETARY

J. William Leonard, Director
Information Security Oversight Office

SUPPORT STAFF

Information Security Oversight Office

SUMMARY OF ACTIVITY

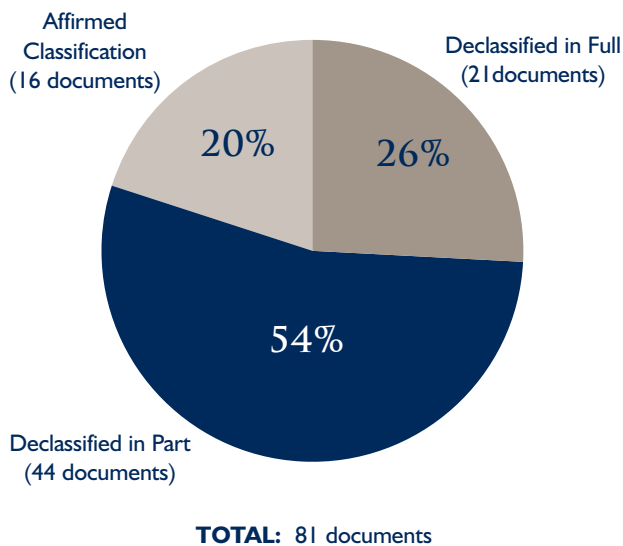
The ISCAP was created under E.O. 12958 to perform the critical functions noted above. The ISCAP, composed of senior-level representatives appointed by the Secretaries of the Departments of State and Defense, the Attorney General, the DCIA, the Archivist of the United States, and the Assistant to the President for National Security Affairs, began meeting in May 1996. The President selects its Chair, the Director of ISOO is its Executive Secretary, and ISOO provides its staff support.

To date, the majority of the ISCAP's efforts have focused on MDR appeals. During FY 2005, the ISCAP decided on 81 documents that remained fully or partially classified upon the completion of agency processing. It declassified information in 80 percent of the documents that it decided upon, declassifying the entirety of the remaining classified information in 21 documents (26 percent), and declassifying some portions while affirming the classification of other portions in 44 of the documents (54 percent). The ISCAP fully affirmed the previous agency decisions in their entirety for 16 documents (20 percent).

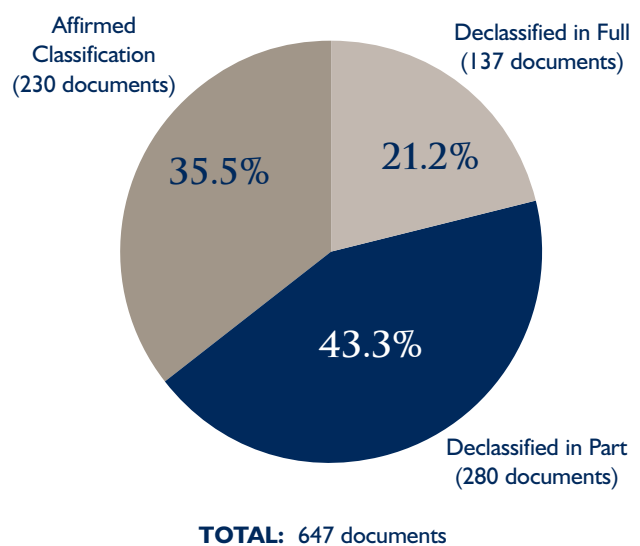
From May 1996 through September 2005, the ISCAP has decided on 647 documents. Of these, the ISCAP declassified information in 64 percent of the documents. Specifically, it declassified the entirety of the remaining classified information in 137 documents (21.2 percent) and declassified some portions while affirming the classification of other portions in 280 documents (43.3 percent). The ISCAP fully affirmed agency classification decisions in 230 documents (35.5 percent).

While the below chart illustrates an increase over time in the percentage of agency decisions affirmed in part or in their entirety by the ISCAP, the shift is the result of a number of factors. For example, the age of the information in individual appeals can affect the ISCAP's decisions. The normal maturation of the standards and principles of E.O. 12958, as amended, throughout the Executive branch, also affects the decisions. As agencies gain experience with the provisions of the amended Order, the ISCAP has seen reduced misapplication of the classification standards when processing MDR appeals. Furthermore, although its decisions are not intended to set precedent, the

ISCAP DECISIONS, FY 2005



ISCAP DECISIONS, MAY 1996–SEPTEMBER 2005



ISCAP's impact on agency positions relative to MDRs is apparent. As set forth elsewhere in this report, MDR processing by agencies results in the declassification, in whole or in part, of more than 95 percent of the pages reviewed. Even after careful and thorough reviews by agencies, it is significant that the ISCAP declassified additional information in 80 percent of the appeals filed.

Between May 1996 and September 2005, the ISCAP heard an appeal of a classification challenge filed pursuant to section 1.8 of E.O. 12958, as amended. This appeal sought to reverse the decision of the Department of the Navy that information within a specific Naval Ship Engineering Center Design Data Sheet was classified. Although the information was more than 25 years old, it concerned "...information that would impair the application of state of the art technology within a U.S. weapon system." The ISCAP affirmed the prior classification of the document under section 3.3(b)(4) of E.O. 12958, as amended.

The ISCAP also approved a declassification guide submitted by the National Reconnaissance Office in accordance with section 3.3(d) of E.O. 12958, as amended, and the applicable provision of its Government-wide implementing directive (32 CFR Part 2001.30(j)). When approved by the ISCAP, such guides authorize the exemption of information determined by an agency to fall within an exemption category listed in section 3.3(b) of E.O. 12958, as amended. Essentially, the guides permit certain information to be classified for more than 25 years. To earn ISCAP approval, a guide must provide the following: (1) a comprehensive description of the information proposed for exemption; (2) a distinct relationship to a specific exemption; (3) a rational justification or explanation of the need for exemption; and (4) a fixed date or event for future declassification.

APPEALS CONCERNING ISCAP DECISIONS

In recognition of the need to hear appeals of agency decisions relating to the MDR program, and because hearing such appeals would place an undue burden on the President, E.O. 12958 established the ISCAP to advise and assist the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. The ISCAP exercises Presidential discretion in its decisions, and it serves as the highest appellate authority for MDR appeals.

The ISCAP's decisions are committed to the discretion of the Panel, unless they are changed by the President. Since its original issuance in 1995, E.O. 12958 has provided agency heads with the ability to appeal the ISCAP's decisions to the President through the Assistant to the President for National Security Affairs. From May 1996 through the amendment of E.O. 12958 in FY 2003, this authority had not been exercised by any agency head; the same is true for FY 2004–05.

However, when E.O. 12958 was amended in FY 2003, the DCI became authorized to block declassification by the ISCAP of certain information owned or controlled by the DCI. Such DCI determinations could be appealed to the President (see section 5.3(f) of the amended Order).

During FY 2003, the DCI blocked the declassification of two documents that the ISCAP had voted to declassify. In both instances, members of the ISCAP appealed the DCI's determination to the President through the Assistant to the President for National Security Affairs. During FY 2004, one of these appeals was rendered moot, as the DCI later declassified the document at issue in its entirety. As of the end of FY 2005, the second appeal remained pending and, thus, the document remains classified in its entirety.

During FY 2005, the DCI did not block the declassification of any information under section 5.3(f) of the amended Order. As noted above, the responsibilities and authorities of the DNI and the DCIA with regard to the ISCAP are currently being addressed.

Documents declassified by the ISCAP may be requested from the entity that has custody of them, usually a Presidential library. For assistance in identifying and requesting copies of such documents, or any other questions, please contact the ISCAP staff at ISOO.

Telephone: 202.357.5250

Fax: 202.357.5907

E-mail: iscap@nara.gov

Additional information about ISCAP can be found on the following page of the ISOO web site:
www.archives.gov/isoo/oversight-groups/iscap

NATIONAL INDUSTRIAL SECURITY PROGRAM

In FY 2005, ISOO finalized the coordination of an implementing directive for E.O. 12829, as amended, “National Industrial Security Program” (NISP). The proposed directive was published in the Federal Register for public comment. After the reconciliation of any feedback and further coordination as necessary, the final directive will be published in the Federal Register. This directive provides additional direction to assist agencies in their NISP implementation.

During FY 2005, a variety of issues continued to inhibit reciprocity in determining eligibility for access to Classified National Security Information. Executive order, statute, and policy explicitly require reciprocity by Executive branch agencies with respect to personnel security clearances to ensure that background investigations are conducted only when they are actually necessary.

E.O. 12968, as amended, “Access to Classified Information,” requires Executive branch agencies to accept adjudications and investigations “mutually and reciprocally,” and allows for an exception only when

the gaining agency has “substantial information” that might adversely affect eligibility. The “Declaration of Principles” promulgated for the NISP in FY 2004 requires reciprocity when a contractor moves from one position to another at the same or lower level of clearance. Intelligence Community Security Implementation Procedure 4-1 from 2004 requires reciprocal acceptance of eligibility determinations for contractors within the intelligence community. The Intelligence Reform and Terrorism Prevention Act of 2004 requires all agencies to accept each other’s investigations and adjudications. It enjoins investigative and adjudicative agencies from creating additional requirements other than polygraph. During FY 2005, E.O. 13381, “Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information,” reiterated the requirement for reciprocity. Also, in December 2005, the Office of Management and Budget (OMB) issued a memorandum for all executive departments and agencies setting forth guidance on procedures to ensure reciprocity.

Nevertheless, reports from industry under the NISP indicate that certain issues remain which inhibit reciprocity. Under E.O. 12829, as amended, the ISOO director, with the agreement of the National Industrial Security Program Policy Advisory Committee (NISPAC) members, has undertaken an initiative to track industry reciprocity among people cleared under the program. This effort fulfills the director’s monitoring responsibilities as chairman of the NISPAC. Data obtained through this trends survey will be reported to the OMB.

ISOO also supported the NISP community through the presentation of workshops on marking and derivatively classifying national security information. It is particularly important that NISP contractors understand their responsibilities in this area to properly apply derivative marking instructions. Correct application will prevent improper derivative classification and unauthorized declassification.

CLASSIFICATION

OVERVIEW

The level of reported classification activity in FY 2005 has dropped for the first time since FY 2001. Increases can still be seen in the Department of Homeland Security (DHS) and the Department of Justice (Justice) as they continue to develop counterterrorism and critical infrastructure protection programs. The number of pages declassified has increased slightly; in spite of a downward trend that has been observed since FY 2001, the number remains higher than the average number of pages declassified annually before the Order's implementation.

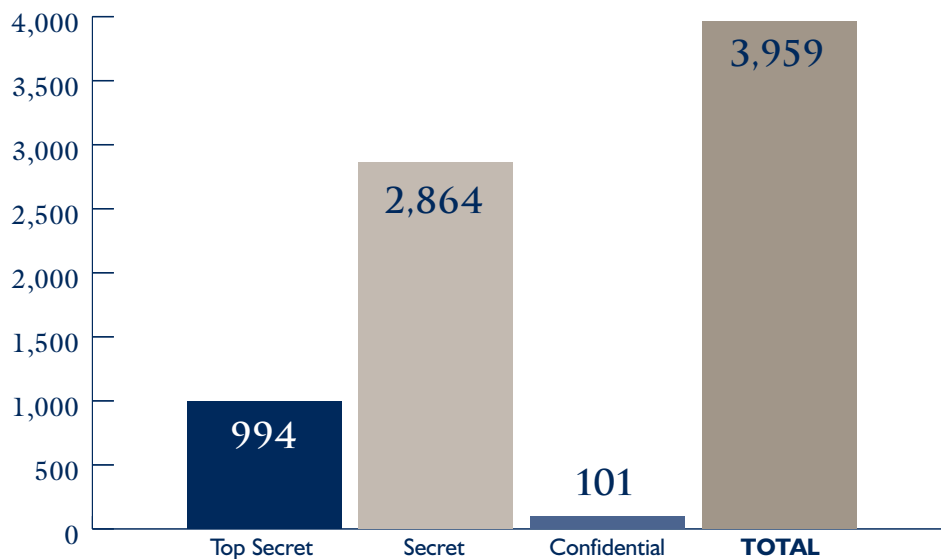
ORIGINAL CLASSIFIERS

Original classification authorities (OCAs), also called original classifiers, are those individuals designated in writing, either by the President or by selected agency heads, to classify information in the first instance. Under E.O. 12958, as amended, only original classifiers determine what information, if disclosed

without authority, could reasonably be expected to cause damage to the national security. Original classifiers must also be able to identify or describe the damage.

There was little net change in the number of OCAs during FY 2005, and the growth in the number of OCAs since FY 2001 appears to be leveling out. Since FY 2001, the creation and development of DHS necessitated an increase in the number of OCAs. In FY 2005, DHS experienced a net loss of two OCAs. FY 2005 saw an influx of 22 new OCAs with the establishment of the Office of the Director of National Intelligence (ODNI), but this was counteracted by reductions in the Department of Defense (DOD) and Justice, which have reduced their number of OCAs by 3 percent and 27 percent, respectively. The net effect was a decrease from 4,007 to 3,959, or 1 percent, in the number of officials with OCA.¹

ORIGINAL CLASSIFIERS, FY 2005



¹ The Office of the Vice President (OVP), the President's Foreign Intelligence Advisory Board (PFIAB), and the Homeland Security Council (HSC) failed to report their data to ISOO this year. Therefore, the reported number of OCAs does not include four OCAs previously reported by OVP and PFIAB. The other data reported here do not include those for OVP, PFIAB, and HSC, which historically have not reported quantitatively significant data.

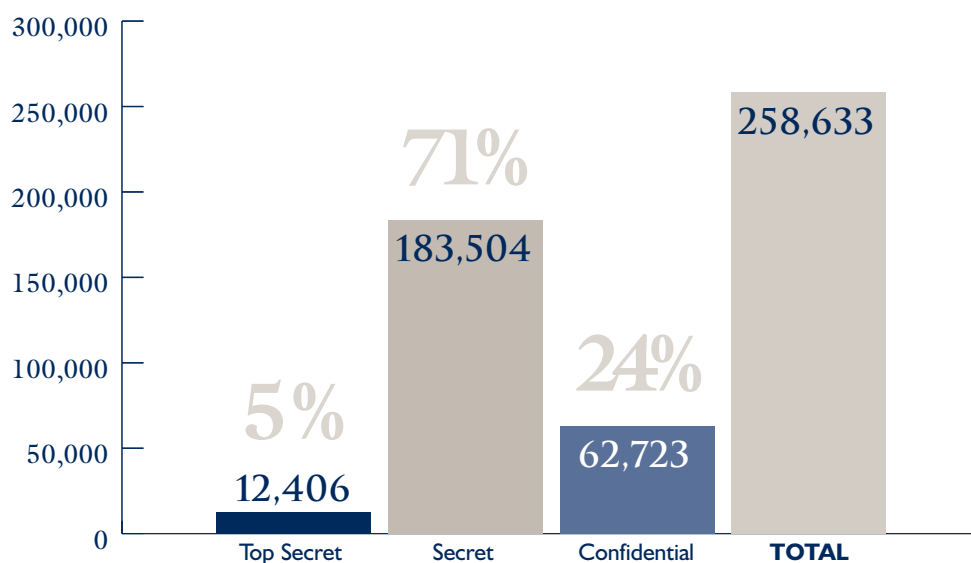
ORIGINAL CLASSIFICATION

Original classification is an initial determination by an authorized classifier that information requires extraordinary protection, because unauthorized disclosure of the information could reasonably be expected to cause damage to national security. The process of original classification always includes a determination by an OCA of the need to protect the information in the interest of national security, the placement of markings to identify the information as classified, a concise reason for the classification, and the date or event when it becomes declassified. By definition, original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification. Simply put, it is the sole source of newly classified information. The derivative category discussed below is the reutilization of information from the original category. Although the derivative category produces many more documents than original classification, it does not produce new classified information (sometimes characterized as “new secrets in the government”). It merely proliferates that which has already been classified.

At best, the derivative numbers provide a rough indicator of how prolific the agencies are in producing information and how much work will need to be done by declassification review teams 20 to 25 years from now. It is, therefore, important to recognize that original classification is a far more significant number on which to focus than derivative. Also, each derivative classification decision must be able to trace its origin back to a decision by an OCA (thus, the primary purpose of the “derived from” line). Derivative decisions that cannot trace their origin or that improperly apply source guidance are a major reason for overclassification.

The numbers reported to ISOO for FY 2005 reveal an estimated 258,633 original classification decisions. This is 92,517 (26 percent) less than what was reported for FY 2004. Most of this decrease came in the Secret and Confidential categories, which are down by 29 percent and 23 percent, respectively. In both of these categories, the most significant decreases were reported at DOD and the Department of State (State), while DHS was up slightly. The Top Secret category did experience a

ORIGINAL CLASSIFICATION ACTIVITY, FY 2005



small increase of 8 percent (971 classification actions), mainly attributable to State and Justice. The overall decrease in original classification is attributed mainly to DOD and State, whose numbers were lower by 29 percent and 33 percent, respectively. The significant decrease in DOD's numbers is reportedly due to a decrease in the number of major operations that required planning and execution. In FY 2004, there were 89 named operations in Iraq, but there were only 46 in FY 2005.

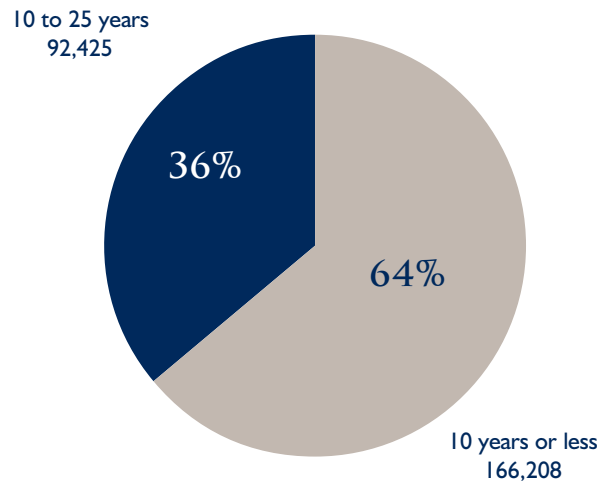
The large decrease from State is directly attributable to the implementation of its classification guide, which was published in FY 2004; however, the majority of State employees have not yet received formal training in the use of the guide. When classification management programs include such guides, the number of original decisions will naturally shift to derivative actions. Because all the original decisions are already specified in the guide, almost all day-to-day classification activity becomes derivative. ISOO sees this as a very positive development, because the proper use of guides, by definition, increases consistency and uniformity in classification determinations, and substantially reduces the probability of inappropriate classification.

As in the case at State, a properly prepared and applied classification guide may prevent derivative classifiers from inappropriately "defaulting" to the assignment of declassification dates that are 25 years from the date of the document. A dramatic positive shift was reported for FY 2005 concerning the assignment of declassification dates on originally classified documents throughout the Executive branch. In FY 2004, only 34 percent of the original classification decisions reported had been assigned a declassification date of less than 10 years from the date

of the document; the FY 2005 data show that this category increased to 64 percent Government-wide.

Historically, under the Order, agencies selected 10 years or less 52 percent of the time in FY 2003; 57 percent of the time in FY 2002; 54 percent in FY 2001; 59 percent in FY 2000; 50 percent in FY 1999; 36 percent in FY 1998; and 50 percent in FYs 1996–97. The FY 2005 data showing 64 percent for the 10-years-or-less category is the highest amount since the Order became effective. ISOO regards this as a positive trend and implores all original classifiers to remember that automatically defaulting to a 25-year declassification date is not in keeping with the Order's direction. Careful thought must be applied to every classification decision with a view to keeping the information classified only as long as absolutely necessary.

DURATION OF CLASSIFICATION, FY 2005



DERIVATIVE CLASSIFICATION

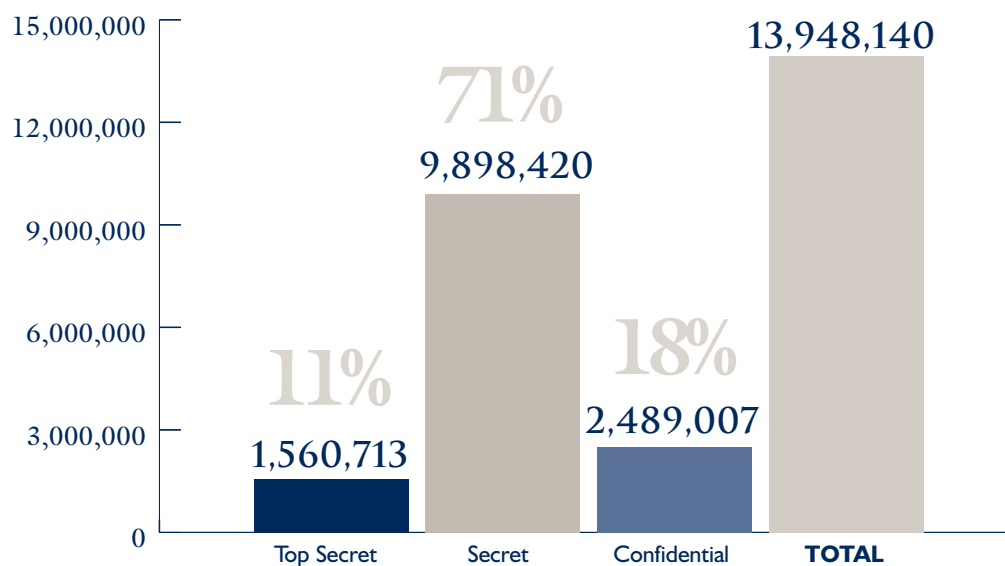
Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form classified source information. Information may be classified in two ways: (1) through the use of a source document, usually correspondence or publications generated by an OCA; or (2) through the use of a classification guide. A classification guide is a set of instructions issued by an OCA. It pertains to a particular subject and identifies the elements of information about that subject that must be classified, as well as the level and duration of classification for each such element. Only employees of the Executive branch or Government contractors with the appropriate security clearance who are required by their work to restate classified source information may classify derivatively.

The agencies reported a total of 13,948,140 derivative decisions in FY 2005, which is a decrease of

1,345,947, or 9 percent, from FY 2004. This decrease was driven mainly by the Central Intelligence Agency (CIA) and DOD, which reportedly were down 5 percent and 20 percent, respectively.

The National Reconnaissance Office (NRO) reported a significant decrease of 23 percent. There were, however, some exceptions to this general decline in derivative numbers. As mentioned above, now that State has begun implementing its classification guide, a significant increase in derivative classification is expected. And, in fact, State did report an overall increase of 222 percent in this category. Justice's derivative actions increased by 7 percent in FY 2005. This upward trend at Justice continues to be attributed to an ongoing expansion of counterterrorism analysis at the Federal Bureau of Investigation (FBI).

DERIVATIVE CLASSIFICATION ACTIVITY, FY 2005

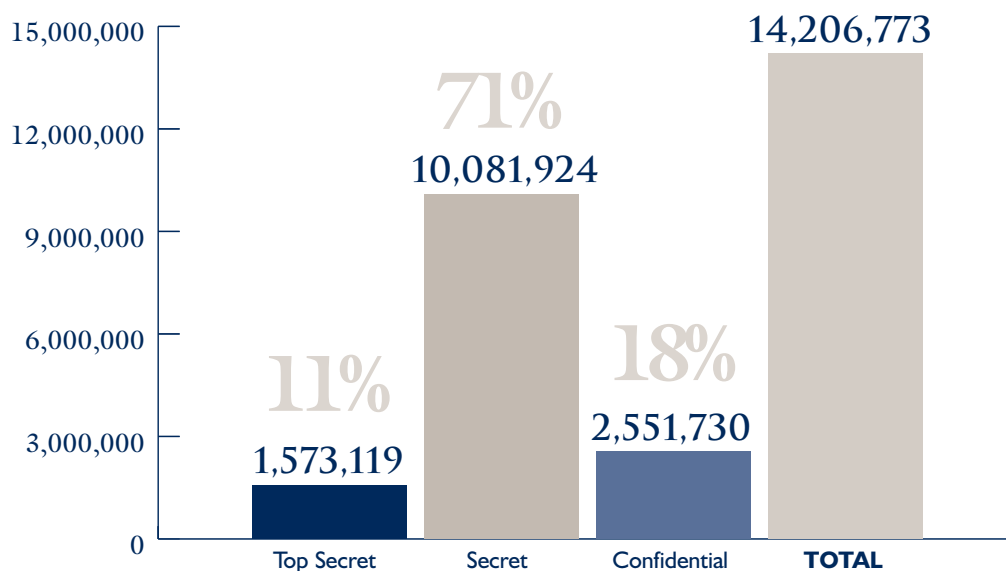


COMBINED CLASSIFICATION

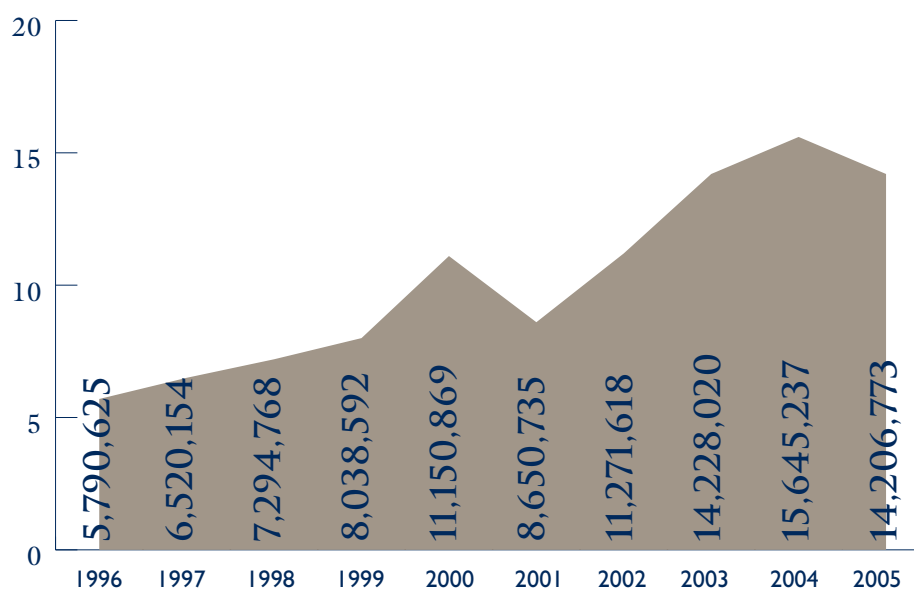
Together, original and derivative classification decisions make up what ISOO calls combined classification activity. In FY 2004, combined reported classification activity totaled 14,206,773 decisions, which is a 9 percent decrease from FY 2003. Judging by the reported numbers, it appears that the Executive branch

agencies, as a whole, are applying better diligence in the management of their information security programs. ISOO views the decrease reported in classification, particularly after three years of rising numbers, as a positive step, but it remains cautious. ISOO will review agency reporting procedures to confirm their reliability.

COMBINED CLASSIFICATION ACTIVITY, FY 2005



COMBINED CLASSIFICATION ACTIVITY, FYs 1996–2005



DECLASSIFICATION

BACKGROUND

Declassification is an integral part of the security classification system. It is the authorized change in status of information from classified to unclassified. When E.O. 12958 was issued on April 17, 1995, there was a paradigm shift in the nation's declassification policies. In preceding years, information once classified remained so indefinitely and very often did not become available to the general public, researchers, or historians without persistent and continuous effort on the part of these individuals. E.O. 12958 changed this paradigm by adding a new "Automatic Declassification" program in addition to the long-standing "Systematic Review for Declassification." Under the automatic declassification provisions of the Order, information appraised as having permanent historical value is automatically declassified 25 years after classification, unless an agency head has determined that it falls within one of several narrow exemptions that permits continued classification, a continuation that either the President or the ISCAP has approved. With the issuance of E.O. 12958, these records were subject to automatic declassification on April 17, 2000.

E.O. 13142, issued on November 19, 1999, amended E.O. 12958, to extend the date of the imposition of the automatic declassification provisions until October 14, 2001. It also extended the date of the imposition of the automatic declassification provisions an additional 18 months, until April 17, 2003, for two groups of records: those that contain information classified by more than one agency and those that almost invariably contain information pertaining to intelligence sources or methods. While Executive branch agencies made significant strides toward meeting the April 17, 2003, deadline, it was clear in late 2001 that this deadline would not be met. As a result, work was begun to further amend the Order to extend the deadline. On March 25, 2003, E.O. 13292 recommitted the Executive branch to the automatic declassification process and extended the date of the imposition of the automatic declassification provision until December 31, 2006. By this date, Executive branch agencies are expected to have completed the declassification of their eligible records

or to have properly exempted them, excluded Restricted Data and Formerly Restricted Data, referred them to other agencies, or, in the case of special media, appropriately delayed declassification. This amendment also reintroduced the concept of exempting, with Presidential approval, a specific file series from automatic declassification, which originally had been a one-time opportunity. In FY 2005 only one file series exemption was approved. Specifically, a file series exemption was approved for certain DOD Special Access Program (SAP) records, resulting in the imposition of automatic declassification not at 25 years but at 40 years for the covered records.

Under Systematic Review for Declassification, which began in 1972, classified permanently valuable records are reviewed for the purpose of declassification after the records reach a specific age. Under E.O. 12356, the predecessor Order, NARA was the only agency required to conduct a systematic review of its classified holdings. Now E.O. 12958, as amended, requires all agencies that originate classified information to establish and conduct a systematic declassification review program, which is undertaken in conjunction with the potential onset of automatic declassification. In effect, systematic review has become an appendage of the Automatic Declassification program. Because they are now interrelated, ISOO collects data on declassification that does not distinguish between the two programs. However, once the first iteration of automatic declassification occurs, ISOO will modify its Standard Form 311 (SF 311), "Agency Security Classification Management Program Data," instructions to distinguish between the two programs.

In effect, E.O. 12958, as amended, reverses the resource burden. Unlike previous systems, in which agencies had to expend resources to declassify older information, under the amended Order, agencies must expend the resources necessary to demonstrate why older historical information needs to remain classified.

FY 2005 marked the 10th year in which the policies leading up to automatic declassification have been in effect.

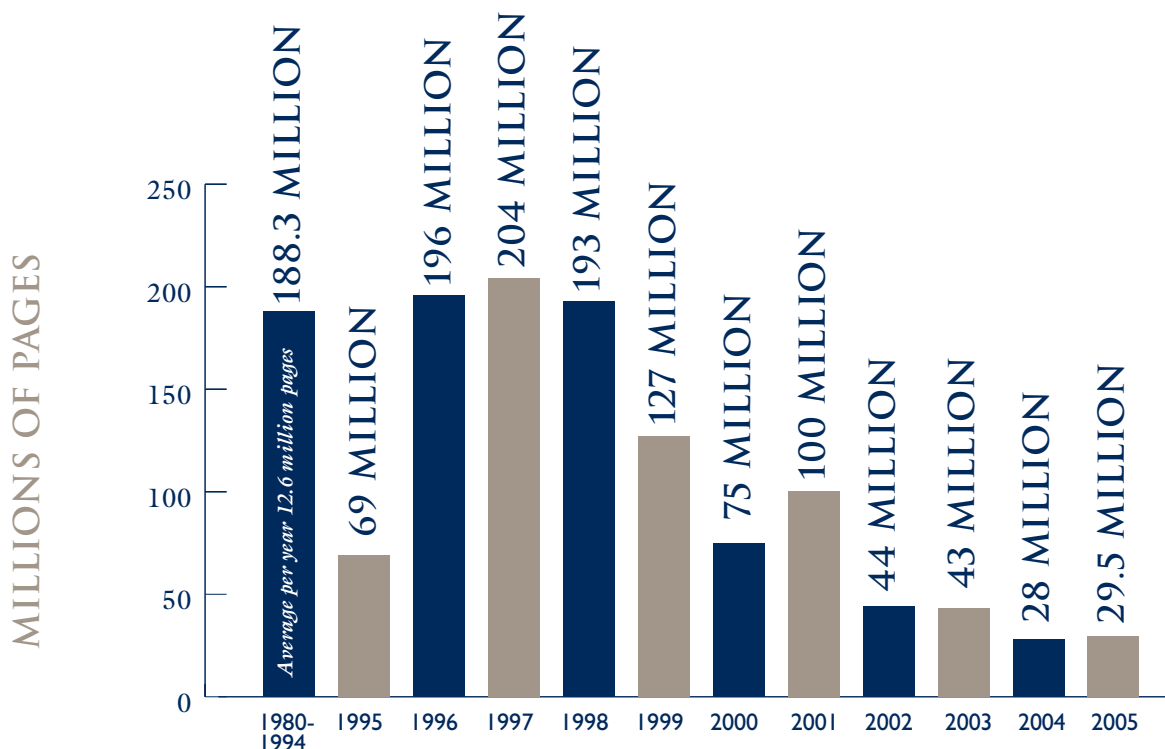
PAGES DECLASSIFIED

During FY 2005, the Executive branch declassified 29,540,603 pages of permanently valuable historical records. This figure represents a 4 percent increase from that reported for FY 2004. This is a small reversal of what has been a downward trend since FY 1997. ISOO realizes that the rate of processing has slowed as a result of several factors, including the increasing complexity of the documents and the number that need to be referred to other equity-holding agencies. Naturally, the time to review, identify, and refer such documents is longer than the time to review a document containing one agency's equity because of the concentrated intellectual analysis and the additional administrative processing time. Despite set-backs experienced by some agencies with respect to funding, and other matters, the number of pages declassified in FY 2005 continues to exceed by more than double the yearly average (12.6 million pages) before the implementation of the automatic declassification provision of this Order.

The number of pages NARA declassified in FY 2005 again declined, from 216,992 pages in FY 2004 to 156,062 pages. In the past four years, NARA's focus has shifted from the actual declassification of other agencies' records to the preparation of records that have been declassified by other agencies for public release.

DOD, whose numbers had previously been declining, reported a 4 percent increase in the number of pages declassified in FY 2005. At this point, DOD is still declassifying more pages than any other agency, accounting for 71 percent of the total. Six other agencies—Department of Commerce (Commerce), Department of Energy (DOE), Department of Transportation (DOT), National Aeronautics and Space Administration (NASA), Nuclear Regulatory Commission (NRC), and National Security Council (NSC)—reported large increases in declassification productivity during FY 2005. Of particular note are Commerce and DOT. Commerce reported 78,080 pages declassified (up from zero). Likewise, DOT

1.3 BILLION PAGES DECLASSIFIED, FYs 1980–2005



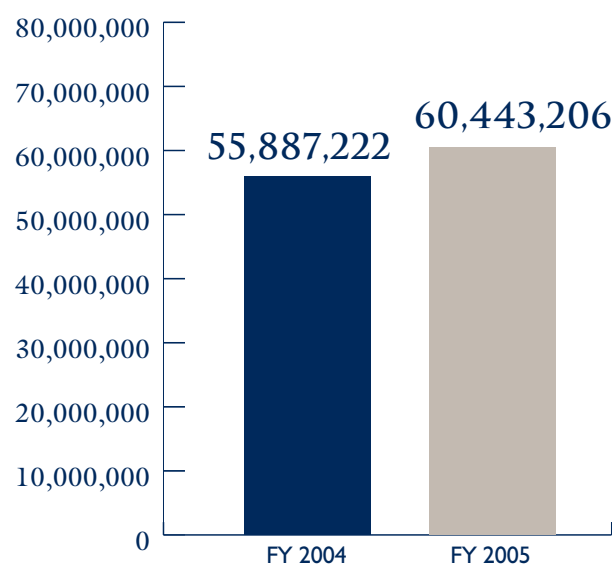
reported 8,000 pages, whereas in previous years it averaged only 18. It is encouraging to see that some agencies are developing robust declassification programs. Four other agencies—CIA, Justice, State, and the U.S. Agency for International Development (USAID)—also reported small decreases in output. ISOO encourages all agencies to sustain or work toward increasing their efforts to implement automatic declassification programs to comply with the December 31, 2006, deadline.

In FY 2004, the agencies reported on the number of pages reviewed, in addition to the number of pages declassified, for the first time. The intent was that this number would provide a better understanding of the level of effort. With the FY 2005 data, ISOO now has two years to compare. In FY 2004, the agencies reviewed 55,887,222 pages; in FY 2005, this number increased by 8 percent to 60,443,206. The overall numbers for both years reveal that agencies are declassifying approximately 50 percent of the pages being reviewed. However, this percentage varies greatly, with some agencies declassifying a much larger percentage and others significantly less. For example, State declassified 90 percent of the pages it reviewed, DOD declassified 62 percent, CIA declassified 26 percent, and DOE declassified 22.5 percent.

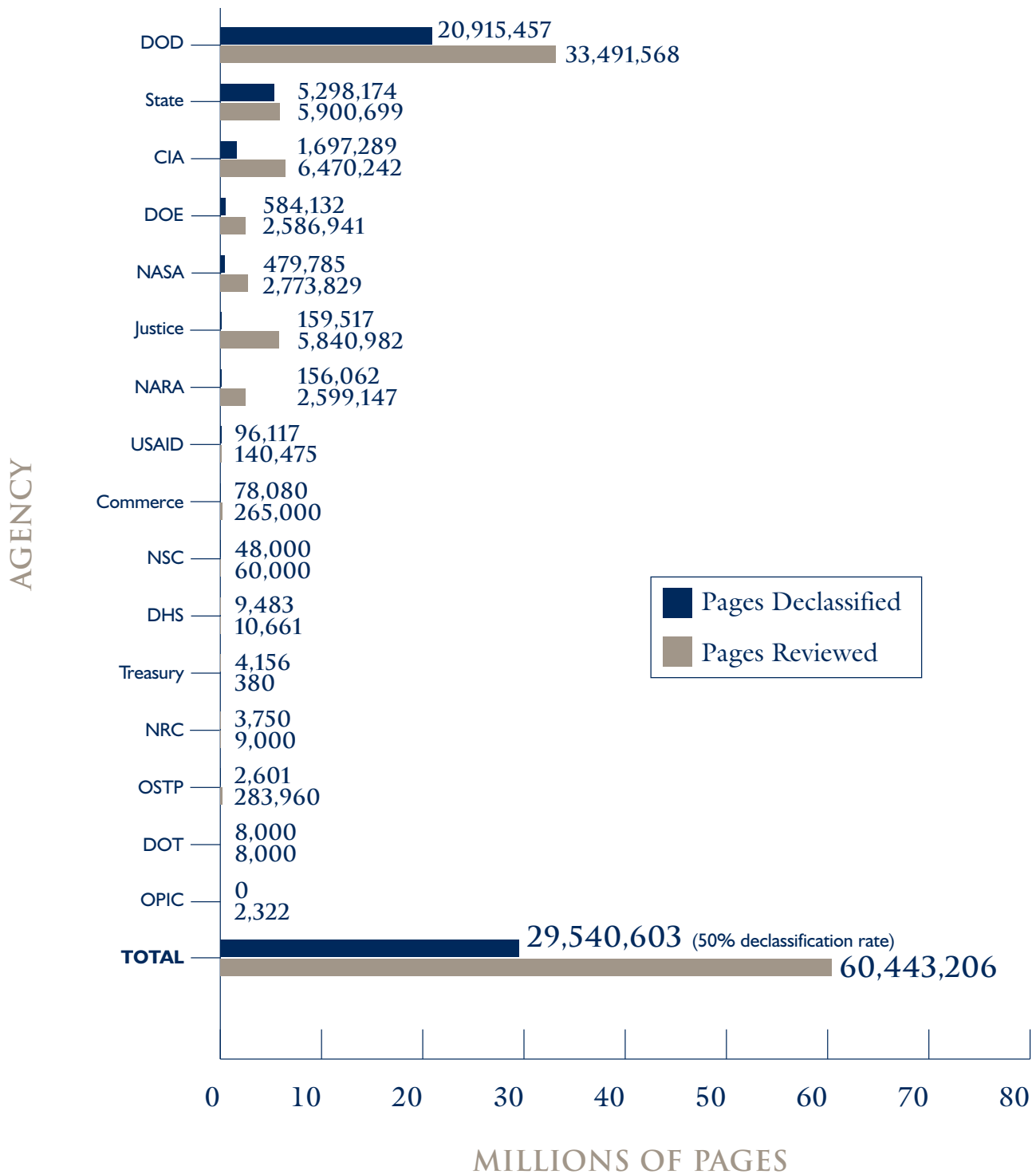
In terms of the total number of pages reviewed in FY 2005, the biggest boost came from Justice, which reported an increase of more than 3 million—more than double its FY 2004 effort. Other agencies with significant increases included Commerce, DHS, DOE, DOT, NARA, and USAID. Commerce and DOT reported the most substantial increases. Commerce reported 265,000 pages reviewed (up from only 394) and DOT reported 8,000 (up from only 23).

In the 10 years that E.O. 12958 has been in effect, Executive branch agencies have reported the declassification of more than 1.3 billion pages of permanently valuable historical records. Compared with the 257 million pages declassified under the previous two Executive orders (E.O. 12065 and E.O. 12356) and before E.O. 12958 became effective, the Executive branch, in the past 10 years, has more than tripled the number of pages it has declassified.

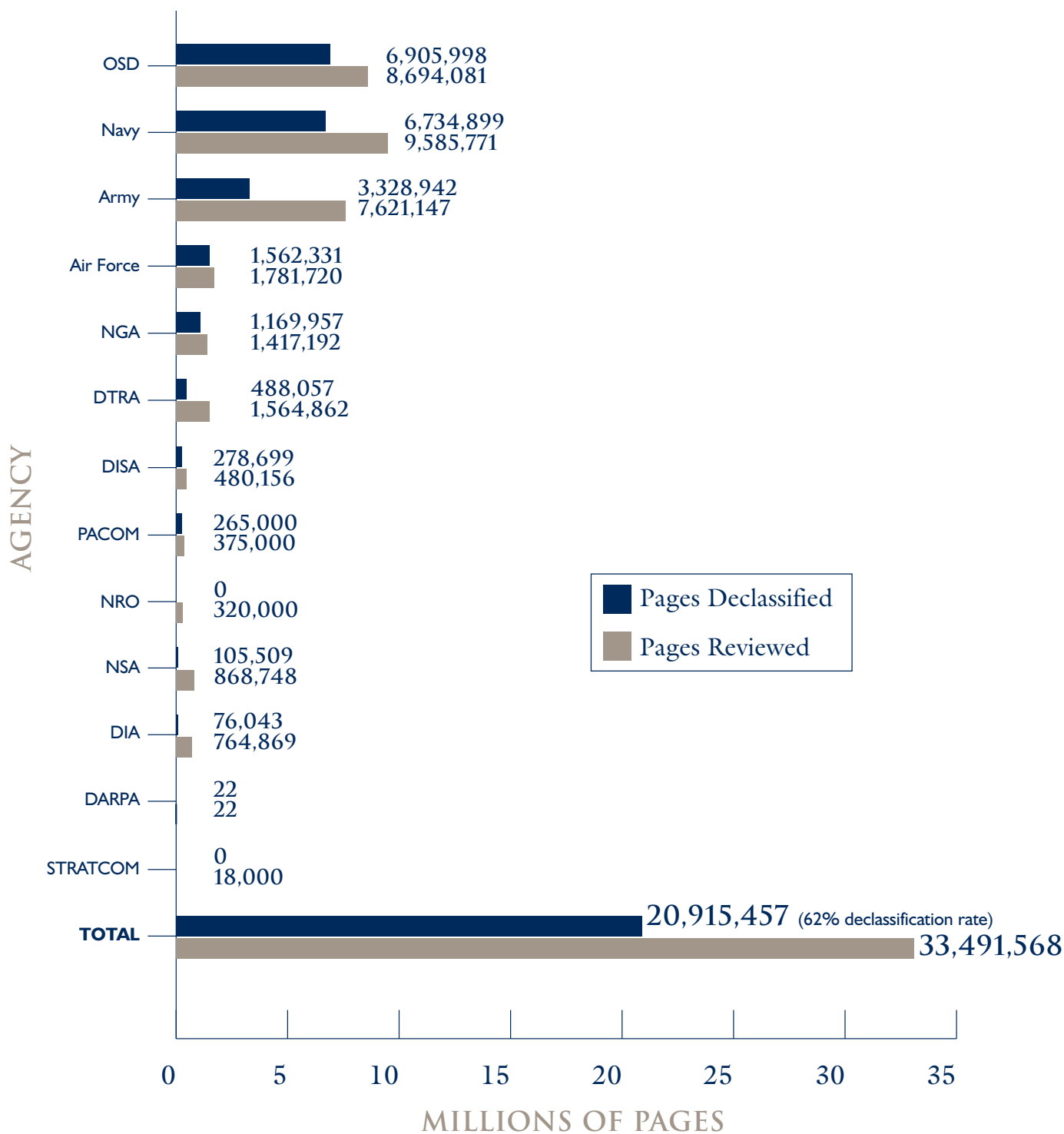
TOTAL NUMBER OF PAGES REVIEWED, FY 2005



NUMBER OF PAGES REVIEWED AND DECLASSIFIED BY AGENCY,
FY 2005



DOD COMPONENTS WITH SIGNIFICANT NUMBERS



PROGRESS TOWARD THE AUTOMATIC DECLASSIFICATION DEADLINE OF DECEMBER 31, 2006

To assess Executive branch progress toward fulfilling the commitment to the December 31, 2006, deadline, ISOO requested that all agencies provide information about their declassification programs to ISOO for review and evaluation. The request was sent to agencies that are original classifiers and/or derivative classifiers, as well as those that are solely consumers or holders of classified national security information.

As of September 21, 2005, ISOO estimates that 155 million pages of classified national security information must be declassified, exempted, or referred to other agencies by December 31, 2006. ISOO believes, for the most part, that the Executive branch is progressing toward fulfilling its responsibilities for these records by the deadline.

Forty-six agencies possessing records subject to section 3.3 of the Order were asked to submit declassification plans. As of September 2005, ISOO was confident that 22 of those agencies will be prepared to implement the Automatic Declassification program by the deadline. Collectively, these 22 agencies account for 39 percent of the total number of pages subject to automatic declassification. ISOO needs to work closely with the remaining 24 agencies to ensure that they allocate sufficient resources to meet the requirement.

The agencies that are on or ahead of schedule with respect to their estimated pages requiring review have several common characteristics, including excellent senior management support, an adequate budget, stable staffing, and a sound review process.

ISOO noted a number of highly effective business practices with respect to implementation of the Automatic Declassification program that warrant special mention. Several agencies have established an organizational structure that ensures careful coordination among their declassification, FOIA, and records management programs. This is a noteworthy best practice that ensures increased efficiency and consistency. ISOO is especially pleased with a number of agencies that have taken leading roles in initiatives,

such as the Interagency Referral Center housed in NARA. Also noteworthy is the CIA's funding and development of the Document Declassification Support System (DDSS), which is now at full operating capability. DDSS is a congressionally mandated, unclassified system for Executive branch agencies to manage the referral process. DDSS is accessible to authorized users via the Internet; it enables agencies to manage and track all referrals, regardless of their physical location.

Another noteworthy organizational approach that has proven successful is the use of a centralized declassification coordinator who oversees all declassification reviews and referrals, regardless of where they may occur within the agency. This facilitates referrals from external agencies and helps ensure that such referrals are directed to the appropriate office of program responsibility.

Another characteristic of the more successful agencies is having a solid working relationship among agency offices of security, declassification, and records management. Such cooperation is evidenced in integrated teams that coordinate, communicate, and resolve issues dealing with classification, declassification, and records management. Declassification oversight committees are especially beneficial in refereeing and resolving conflicts regarding difficult release decisions.

Agencies that have less successful programs and risk missing the deadline have inadequate senior management support, under-funded budgets, fewer well-trained staff, high personnel turnover rates, and little or no process for reviewing or coordinating records. A secondary factor for several agencies is that they are only now starting the process of identifying records for review.

ISOO will continue to work with all agencies and offer what assistance it can to keep the process moving forward. ISOO has emphasized to each agency head that automatic declassification is an ongoing program that begins, not ends, on December 31, 2006.

MANDATORY DECLASSIFICATION REVIEW

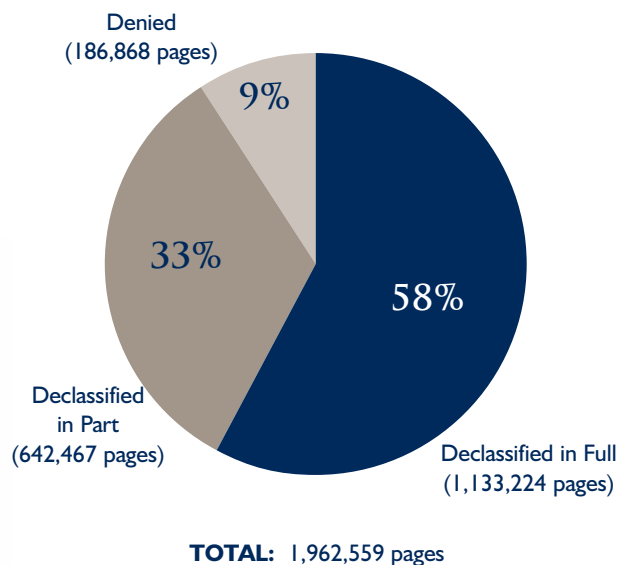
Under E.O. 12958, as amended, the MDR process permits individuals or agencies to request the review of specific national security information for the purpose of seeking its declassification. Requests must be in writing and must describe the information with sufficient detail to permit retrieval with a reasonable amount of effort. MDR remains popular with some researchers as a less contentious alternative to requests under FOIA, as amended. MDR is also used to seek the declassification of Presidential papers or records not subject to FOIA.

INITIAL REQUESTS

Agencies processed 3,517 initial requests for MDR during FY 2005. This represents a decrease of 953 requests from FY 2004, and is below the 3,834 average number of initial requests for MDR processed annually for FYs 1996–2004. The total number of pages processed during FY 2005 was 150,660. This represents a decrease of 153,715 compared with FY 2004 and is significantly less than the average number of pages (184,242) processed annually for FYs 1996–2004.

The processing of initial requests for MDR during FY 2005 resulted in the declassification of information in 137,312 pages, or 91 percent of the pages processed. Specifically, it resulted in the declassification of 66,569 pages in full (44 percent) and 70,743 pages in part (47 percent). Nine percent, or 13,348 pages, remained classified in their entirety after being reviewed. As demonstrated below, MDR remains a successful means of declassifying information, resulting in information being declassified in 91 percent of the pages processed from FYs 1996–2005.

DISPOSITION OF INITIAL MDR REQUESTS, FYs 1996–2005



APPEALS

During FY 2005, agencies processed 152 appeals of agency decisions to deny information during the processing of initial requests for MDR. This represents a slight decrease from FY 2004, during which agencies processed 163 MDR appeals. FY 2005 represents the third-largest number of MDR appeals processed in a single fiscal year since the issuance of the Order and is well above the average of 101 appeals processed annually for FYs 1996–2004. Agencies processed 8,863 pages as part of these MDR appeals, representing a significant increase over the 2,729 pages processed in FY 2004 and the average of 3,769 pages processed annually for FYs 1996–2004. In fact, FY 2005 represented the largest number of pages

processed under MDR appeal since the Order was issued in FY 1996.

The processing of MDR appeals by agencies during FY 2005 resulted in the declassification of information in 2,720 pages, or 31 percent of the pages processed. Specifically, it resulted in the declassification of 1,202 pages in full (14 percent) and 1,518 pages in part (17 percent). Sixty-nine percent, or 6,143 pages, remained classified in their entirety after being reviewed.

As the chart above demonstrates, information is often declassified on appeal, suggesting that requesters can anticipate greater returns in declassified information if they pursue an appeal.

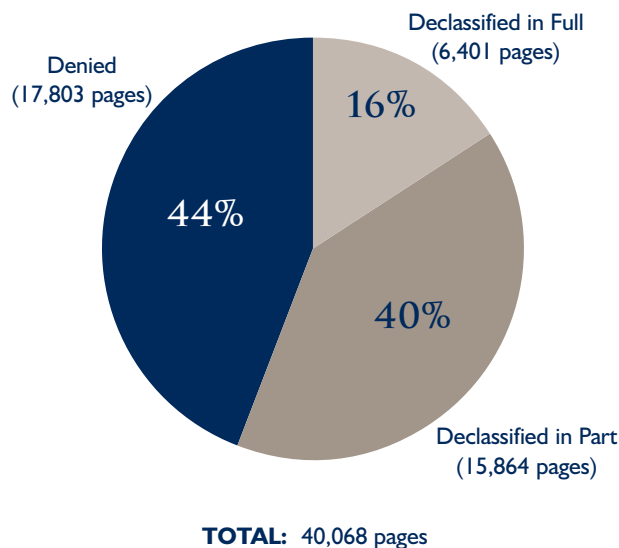
Any final decision made by an agency to deny information during an MDR appeal may be appealed by the requester directly to the ISCAP. The agency is required by E.O. 12958, as amended, to notify the requester of these appeal rights. Should an agency fail to meet the time frames indicated in Article VIII, section A(3) of Appendix A to 32 CFR Part 2001, agencies, requesters, and appellants should be aware that initial requests for MDR, and MDR appeals, may be appealed directly to the ISCAP.

Additional information about MDR can be found in: (1) sections 3.5 and 3.6 of E.O. 12958, as amended; (2) 32 CFR Part 2001.33; and (3) Article VIII of Appendix A to 32 CFR Part 2001. Please consult the following page on the ISOO web site: www.archives.gov/isoo/oversight-groups/iscap/mdr-appeals.html

If you have any questions concerning MDR, please contact the ISCAP staff at ISOO:

Telephone: 202.357.5250
Fax: 202.357.5907
E-mail: iscap@nara.gov

DISPOSITION OF MDR APPEALS, FYs 1996–2005



MDR SPECIAL REVIEW

OVERVIEW

MDR is a means by which any individual can request an agency to review a classified record for declassification, regardless of its age or origin, subject to certain limitations set forth in E.O. 12958, as amended. The vast majority of such requests result in the declassification and release of previously classified information. The process often proves fruitful for requestors of previously withheld government information, in part, because of the built-in appeal rights requestors have, both internal and external to the agency responsible for the classified information. Unlike requests made pursuant to FOIA, for example, after individuals exhaust their MDR appeal rights in an agency, they have the right to make an additional administrative appeal of an agency's decision with ISCAP. More often than not, an appeal to ISCAP, which takes a broader view than that employed by the originating agency, will result in the declassification of additional information.

To increase its understanding of the MDR program in Executive branch agencies and to enhance its oversight of the Government-wide program of nearly 80 agencies and entities with classified information security programs, ISOO initiated a series of special on-site reviews. These reviews were initiated to analyze the MDR program regulations and guidance, review the process for both initial requests and appeals, and collect and analyze statistical data for FYs 1996–2003. The project involved on-site reviews of the MDR programs at eight agencies, including the Department of the Army (Army), CIA, NARA, NASA, the National Security Agency (NSA), the Office of the Secretary of Defense (OSD), State, and the Department of the Treasury (Treasury). These eight agencies, which reflect a cross-section of civilian, defense, and intelligence agencies, have the largest volume of MDR activities.

ISOO also conducted interviews with several members of the general public, representing the researcher and historian communities, which routinely request the declassification of national security information through the MDR program or FOIA. This report summarizes these findings and provides recommendations for ISOO and the Executive branch as a whole to improve the MDR program.

RESULTS

At a minimum, under the MDR provisions of the Order, agency heads are required to develop procedures to promptly process MDR requests, notify requesters of results, and provide means for administrative appeals of denials, which includes notifying requesters of the right to appeal a final agency decision to ISCAP. Overall, ISOO found that none of the eight sampled agencies fulfilled all of the requirements under the Order and its implementing directive. Deficiencies were exhibited in the following categories: (1) current and compliant regulations; (2) publication in the Federal Register of MDR contacts; (3) current internal procedures to provide for initial requests and appeals; (4) timeliness of responses; and (5) internal oversight through the self-inspection program.

Only two of the eight agencies reviewed had current, final regulations regarding their MDR program, and four had final regulations in place that needed to be updated to fully reflect the 2003 amendment to the Order. For example, several agencies failed to mention time frames for initial requests, provided incomplete information about appeal rights, or incorrectly required citizenship as a criterion for filing a request. The two remaining agencies have interim MDR regulations that are being updated to include a section on appeals. The review and analysis of the remaining Executive branch agencies that ISOO oversees is discussed later in this report.

Seven of the eight agencies had MDR point of contact (POC) information published in the Federal Register as required by the Order. Only two of the agencies posted current information. Although the information for five of the agencies is outdated, only one of these five had indicated that it is in the process of updating its information. Although not required under the Order, five of the agencies cited the MDR POC information separately or under their FOIA web site contact information. Posting POC information on an agency's web site was noted during general public interviews as the most effective way to convey contact information about an agency's MDR program office or personnel.

All agencies must have MDR procedural guidance in place to be used by staff and requesters for initial requests and appeals. As confirmed during the on-site reviews, seven of the eight agencies had procedures in place regarding initial processing. Of these, six of the agencies' procedures were adequate and in compliance with the Order. The seventh needs to update its internal regulations to be in compliance with the 2003 revisions to the Order, and the eighth agency must establish MDR procedural guidance.

Regarding internal procedures governing the appeals process, only three of the agencies had appeal procedures in place that were fully compliant with the Order. Five of the eight agencies are less than fully compliant. Two agencies had procedures in place, but they were not adequate and require revision to protect the requester's rights. Three agencies had no administrative or ISCAP appeal procedures in place.

Agencies are further required to establish internal self-inspection programs to include MDR program reviews. None of the agencies included MDR as part of its ongoing self-inspection program. ISOO noted in the MDR program review letters to the senior agency officials of the eight selected agencies that it would continually evaluate MDR programs in ongoing agency reviews and stressed that each agency was required to include MDR in its self-inspection program.

The review of statistical data reported to ISOO by Executive branch agencies on SF 311 for FYs 1996–2003 yielded the most significant findings. First, in its *FY 2004 Annual Report*, ISOO indicated that, Government-wide, an annual average of 3,874 MDR requests were initiated during FYs 1996–2003. On the basis of an analysis of the data and interviews with the eight agencies, ISOO determined that this number was greatly inflated because of a misunderstanding about how to report MDR cases. Most of the initial requests come through NARA's Presidential library system or NARA's Office of Records Services and were then referred to another agency for a decision on equities contained in the document. Other than NARA, each agency had a low number of initial MDR requests; nearly all should have been reported as referrals. As a result of this finding, ISOO must provide better guidance in its SF 311 data collection instructions to ensure that agencies properly report the number of initial requests rather than NARA referrals. Moreover, ISOO will review the data elements and instructions and take action to ensure that it obtains accurate information about the processing of initial requests, appeals, and referrals.

Second, several of the agencies interviewed have been making a concerted effort to reduce the

backlog of MDR cases in their queues, most of which are referrals. ISOO commends those agencies for their efforts. However, these efforts spotlight a major flaw in the MDR program; that is, timeliness of MDR processing. It appears that some agencies have failed to allocate sufficient resources or have otherwise not effectively used available resources to provide timely responses to MDR requests, appeals, and referrals. This is unacceptable.

Of particular concern is the ever-increasing backlog of initial MDR requests that are being received by NARA but are not being processed in a timely manner. ISOO has encouraged NARA to improve its process to avoid excessive delays, particularly in light of the impact NARA's program has on other Government agency programs. ISOO has asked NARA to review the resources allocated to, and the processes used in, its MDR program to ensure that MDR cases, initial referrals, and appeals are processed in a timely manner. Indeed, ISOO asks that all Executive branch agencies perform this same review of their processes and resources so that their MDR programs are in compliance with the requirements of the Order and its directive.

As reported earlier, ISOO monitors nearly 80 Executive branch agencies in its oversight capacity. Of these agencies, 28 are in the Defense Group and governed first by DOD Directive 5200.1-R, "DOD Information Security Program," which has been issued as an interim directive. Until the DOD regulation is finalized, the Defense agencies should follow this guidance. Of the remaining agencies that ISOO oversees, 20 small agencies have little or no information security activities and no MDR program regulations, 15 large agencies have no updated regulations, and 5 agencies have current and complete MDR regulations. All other agencies are covered under other agencies' regulations.

As noted above, ISOO conducted interviews with several members of the general public representing the researcher, historian, and FOIA communities. These include members of an independent non-Government research institute, a prominent historian, a frequent ISCAP requester, and an attorney who specializes in national security, foreign sovereignty and diplomatic immunity, and FOIA litigation. All public-sector interviewees were familiar with, but had varied experience with, the Government-wide MDR program. Overall, they have low expectations for the effectiveness of MDR in fostering declassification and release of national security information, and they share a mistrust regarding the attention the agencies pay to

MDR requests and the agencies' determinations to declassify information. They believe that the Government, as a whole, is not fully publicizing MDR program information to the American people. However, the two persons who had appealed at the agency level and elevated their MDR requests to the ISCAP were satisfied with the outcome of that body's declassification decision.

ISOO found that public and Government participants in the program review could benefit generally from a full understanding of the MDR program, training, and outreach, and an understanding that much of the work is in the Presidential libraries and dependent on their resources to move requests forward. The MDR review participants viewed the MDR program as a subset of FOIA, wanted ISCAP deliberative process and decisions publicly released, and expected ISOO intervention and guidance.

CONCLUSIONS

Based on its program review, ISOO has or will carry out and monitor the following steps and action items to reinforce the overall state of the MDR program in the next few months:

- Post Executive branch agency MDR POC information on the ISOO web site and update as necessary, add links to agency MDR web sites, and revise general MDR information on the ISOO web site, as appropriate.
- Request that all Executive branch agencies review and update their MDR regulations, internal procedures, and POC information. ISOO will request that these agencies develop an MDR program information section on their public web sites similar to the section devoted to FOIA.
- Request NARA, including the Presidential libraries, to coordinate with other agencies to foster a uniform and timely MDR referral process.
- Provide additional data collection instructions for completing the SF 311, sections E and F (MDR). In the short term, ISOO will request specific information regarding initial requests, appeals, and referrals as an additional requirement in the comments line until the SF 311 is formally modified to include these new data fields.
- Require that all agencies incorporate MDR program reviews as part of their self-inspection programs and include oversight of agency MDR programs in all ISOO program reviews.
- Remind agency heads and senior agency officials of their responsibilities under section 5.4 of the Order with respect to MDR and oversee agency allocation of sufficient personnel and resources for effective MDR programs.
- Submit letter reports to the eight agencies notifying them of ISOO findings. Include action items and offer liaison assistance to assist agencies in meeting MDR compliance requirements.
- Develop and distribute an MDR brochure and flowchart outlining a step-by-step process for requesters, appellants, and agencies. Identify, develop, and provide other MDR promotional products.

Through these means and others, ISOO will continue to assist agencies and individuals, and increase its oversight to ensure a compliant MDR program Government-wide.

PUBLIC INTEREST DECLASSIFICATION BOARD

INTRODUCTION

In establishing the Public Interest Declassification Board (PIDB), Congress and the President determined that it is in the national interest to establish an effective, coordinated, and cost-effective means by which records on specific subjects of extraordinary public interest that do not undermine the national security interests of the United States may be collected, retained, reviewed, and disseminated to policy makers in the Executive branch, Congress, and the public.

PURPOSE

- Advises the President and other Executive branch officials on the systematic, thorough, coordinated, and comprehensive identification, collection, review for declassification, and release of declassified records and materials that are of archival value, including records and materials of extraordinary public interest.
- Promotes the fullest possible public access to a thorough, accurate, and reliable documentary record of significant U.S. national security decisions and significant U.S. national security activities to—
 - support the oversight and legislative functions of Congress;
 - support the policy-making role of the Executive branch;
 - respond to the interest of the public in national security matters; and
 - promote reliable historical analysis and new avenues of historical study in national security matters.
- Provides recommendations to the President for the identification, collection, and review for declassification of information of extraordinary public interest that does not undermine the national security of the United States.
- Advises the President and other Executive branch officials on policies deriving from the issuance by the President of Executive orders regarding the classification and declassification of national security information.
- Reviews and makes recommendations to the President with respect to any congressional request, made by the committee of jurisdiction, to declassify certain records or to reconsider a declination to declassify specific records.²

² Responsibility added by Section 1102 of the Intelligence Reform and Terrorism Prevention Act of 2004, which also extended the sunset clause of the Board to December 31, 2008.

MEMBERSHIP

The Board is composed of nine individuals appointed from among citizens of the United States who are preeminent in the fields of history, national security, foreign policy, intelligence policy, social science, law, or archives. The following are the members as of the end of FY 2005:

L. Britt Snider, Chair, appointed for a four-year term by the President in October 2004

Martin Faga, appointed for a four-year term by the President in October 2004

Steven Garfinkel, appointed for a four-year term by the President in October 2004

Joan Vail Grimson, appointed for a three-year term by the Majority Leader of the U.S. Senate in March 2005

Elizabeth Rindskopf Parker, appointed for a three-year term by the President in October 2004

David Skaggs, appointed for a two-year term by the Minority Leader of the U.S. House of Representatives in January 2005

Richard Norton Smith, appointed for a two-year term by the President in October 2004

As of the end of FY 2005, two appointments were pending (one from the Speaker of the U.S. House of Representatives and one from the Minority Leader of the U.S. Senate).

The Director of the ISOO serves as the Executive Secretary to the Board, and the ISOO staff provides support.

UPDATE

The inaugural meeting of the PIDB was held in Washington, D.C., on February 25, 2006; a subsequent meeting was held on April 1, 2006. Specific coverage of PIDB activities will be included in future ISOO Reports to the President.

If you have any questions concerning the PIDB, please contact the PIDB staff at ISOO:

Telephone: 202.357.5250

Fax: 202.357.5907

E-mail: pidb@nara.gov

REVIEWS

SUMMARY OF ACTIVITY

In FY 2005, pursuant to section 5.2(b)(4) of E.O. 12958, as amended, ISOO conducted a total of 25 on-site reviews of Executive branch agencies. Among these were 18 general program reviews of civilian, intelligence, and military agencies of varied sizes. The general reviews evaluated the agencies' implementation of the classified national security information program to include such core elements as organization and management, classification and declassification, security education and training, self-inspections, safeguarding practices, and security violation procedures. ISOO also conducted seven special program reviews focused specifically on declassification procedures and practices. Six evaluated agency declassification activities, and one measured the presence of other agency equities in a particular agency's 25-year-old classified records of permanent historical value.

GENERAL PROGRAM REVIEWS

The ISOO program reviews found that most of the 18 agencies have adequately implemented the majority of the core elements of the classified national security information program. A few of these programs were excellent, but most needed improvement in one or more areas. Shortcomings were observed at multiple agencies in their self-inspection programs, implementing regulations, and refresher security education and training. It is disappointing that these same shortcomings were noted in the ISOO FY 2004 Annual Report. At one agency, the ISOO on-site review revealed a significant incident involving the spillage of national security information classified at the Secret level into an unclassified information system exposed to the Internet.

As found in FY 2004, many agencies have not established comprehensive self-inspection programs. Seven agencies had no self-inspection programs, and seven agencies' self-inspection programs did not include a periodic review of their classified product, as required by section 5.4(d)(4) of the Order. The primary reasons for the shortcomings of these

agencies' self-inspection programs included inadequate staffing levels needed to meet internal oversight responsibilities and insufficient emphasis by senior agency officials. Self-inspections are an important element of the information security program, because they enable the agency to evaluate, as a whole, its implementation of the Order's program and to make adjustments and take corrective action, as appropriate.

Another area of concern was the failure of agencies to update their regulations that implement E.O. 12958, as amended. Seven agencies had not implemented revised regulations, although the Order was amended in 2003, and one agency did not have an implementing regulation as required under the Order. Implementing regulations are essential to the program because they are the foundation for agency personnel to obtain guidance for and procedures pertinent to their individual responsibilities under the Order and ISOO Directive No. 1.

Refresher security education and training, although an annual requirement of the Order, was not being provided at six of the agencies reviewed. This training is fundamental to the continuous reinforcement of the policies, principles, and procedures that clearance holders are expected to understand and implement.

With the continued and ever-increasing interconnection of information systems, the extent and risk of classified information spillage has become a Government-wide challenge. In addressing the incident revealed in the on-site review, ISOO provided guidance to contain and prevent further spillage of classified information into the unclassified system; to isolate and protect the classified information from unauthorized disclosure; and for a risk management-based decision regarding the maintenance of operations. ISOO's oversight in this area enhanced its knowledge and helped it to develop formal policy and guidance for such incidents through the Classified Information Spillage Working Group under the auspices of the Committee on National Security Systems.

DOCUMENT REVIEWS

An assessment of agencies' classified product is an important element of ISOO reviews. ISOO examined classified documents during the general program reviews to evaluate the application of classification and marking requirements of the Order. At the 18 agencies, ISOO reviewed a total of 2,099 documents and found discrepancies in 878 documents (41.8 percent). There were a total of 1,389 discrepancies, which is an average of 1.58 discrepancies in each of the documents that contained errors, yielding an error rate of 66 errors per 100 documents. The most frequently occurring discrepancies included the use of improper declassification instructions, the inconsistent application of portion markings, and a failure to indicate the basis for classification of the documents. Nearly 22 percent of the documents had declassification instruction errors. The most common error was the continued use of the X1 through X8 exemptions, which have been invalid since the amendment to E.O. 12958 in 2003. Portion markings were inconsistently applied in more than 17 percent of the documents.

Of paramount concern were those documents (10.6 percent) whose basis for classification could not be traced to an OCA, which is an essential requirement of the Order's program. The program mandates this requirement through its provision to include a "Classified By" or "Derived From" line on every classified document. Because these documents lacked this information, ISOO could not determine the basis for their classification, thus making the appropriateness of their classification status uncertain. The consequences of this shortcoming are considerable. Because of the uncertain classification status of the sources, any future classification decisions based on these documents will be problematic.

CONCLUSIONS

The elements of the agencies' classified national security information programs are interdependent. These implementing regulations set the foundation for the program and establish the agency's framework to implement the Order. Deficiencies in regulations lead to gaps in the agency's program implementation. Security education and training briefings inform agency personnel on their duties and responsibilities and on the proper procedures for creating, handling, and destroying classified information. Personnel with insufficient training are more prone to make mistakes while working with classified information. Self-inspections enable an agency to evaluate its program implementation on a regular basis, identify areas of concern, and take corrective action, as applicable. The absence of a self-inspection program can leave problems unidentified and uncorrected.

An example of the interrelationship of these elements can be seen in the marking of classified documents. Agency implementing regulations must reflect the marking requirements of the current Order. Agency personnel must be properly trained on the marking of the documents. Agency self-inspections that include a review of the classified product will identify marking discrepancies, should they exist. The high error rate in the documents reviewed can only be addressed by a multifaceted effort that includes a review and update, as necessary, of implementing policies and procedures; a dedicated ongoing training effort; and regular, continuous oversight of the classified product that is produced.

Spillage of classified information into unclassified information systems or higher-level classified information into lower-level classified information systems, including non-Government systems, remains a Government-wide problem. It is caused by the continued and ever-increasing interconnection of systems, especially through web-based and Internet technologies. In addressing such incidents, agencies must make risk management decisions that safeguard and protect classified information while balancing the need to maintain operations.

SPECIAL PROGRAM REVIEWS (DECLASSIFICATION)

Between March and August 2006, ISOO conducted special on-site reviews of six major classifying agencies to evaluate their use of declassification guides, their application of file series exemptions, and their ability to track referrals they receive from other agencies. ISOO reviewed declassified documents to determine whether agencies understood declassification guidance and whether they were properly applying it. Of the agencies reviewed, two had received final approval from ISCAP for their declassification guides and were properly applying the guidance. Four agencies had interim approval for their guides, and their application was deemed to be appropriate upon final approval. Four of the agencies had received approval from the President for file series exemptions; one was seeking approval; and, for one, file series exemptions were not applicable at the time of the review. One agency was improperly applying its file series exemptions. A file series exemption applies to a specific body of records for which automatic declassification review has been delayed until an agreed-on date (e.g., 10, 25, or 50 years). It may not be applied to individual records located in other file series. This agency was applying the file series exemptions as if they were exemptions approved by the ISCAP in a declassification guide. In the area of referrals, two of the agencies had some difficulty locating records that had been referred to them.

ISOO conducted an additional declassification review at an agency to identify other agency equities in the agency's documents. ISOO wanted to demonstrate the necessity of a declassification review even if the agency was willing to release all of its own information. ISOO reviewed a random sample of 324 documents in files at the agency and in agency records accessioned into NARA. ISOO found that more than 70 percent of the documents contained other agency equities. Since the ISOO review, the agency has taken steps to review its records to ensure that other agency equities are identified and the agencies are notified.

CONCLUSIONS

The results of these ISOO special reviews confirmed concerns that ISOO had identified and has been working to address throughout the Executive branch. Agencies that determine the need to continue the classification of information beyond 25 years must meet the requirements of the Order and gain approval of the ISCAP for exemption of the information, usually in the form of a declassification guide. For all records predating 1982, such requests must be received no later than June 30, 2006. For records predating 1982, agencies that need to request a Presidential file series exemption to delay the review of classified information for a specific amount of time must submit requests as soon as possible. ISOO has made these requirements clear to the agencies, and ISOO program analysts have been working with agency counterparts to assist in the preparation and submission of declassification guides and file series exemption requests. ISOO has been working with agencies—through the Remote Archives Capture (RAC) Program, the External Referral Working Group (ERWG), the Classification Management Working Group (CMWG), and other projects, organizations, and committees—to ensure that notifications of referrals contain all pertinent information. This will ensure a timely review of the referred equities by all agencies by the deadline of December 31, 2009, and each year thereafter.

AGENCY ACRONYMS AND ABBREVIATIONS

Air Force:	Department of the Air Force	NISPAC:	National Industrial Security Program Policy Advisory Committee
Army:	Department of the Army	NRC:	Nuclear Regulatory Commission
CEA:	Council of Economic Advisers	NRO:	National Reconnaissance Office
CIA:	Central Intelligence Agency	NSA:	National Security Agency
Commerce:	Department of Commerce	NSC:	National Security Council
DARPA:	Defense Advanced Research Projects Agency	NSF:	National Science Foundation
DCAA:	Defense Contract Audit Agency	OA, EOP:	Office of Administration, Executive Office of the President
DCMA:	Defense Contract Management Agency	ODNI:	Office of the Director of National Intelligence
DeCA:	Defense Commissary Agency	OIG, DOD:	Office of the Inspector General, Department of Defense
DFAS:	Defense Finance and Accounting Service	OMB:	Office of Management and Budget
DHS:	Department of Homeland Security	ONDCP:	Office of National Drug Control Policy
DIA:	Defense Intelligence Agency	OPIC:	Overseas Private Investment Corporation
DISA:	Defense Information Systems Agency	OPM:	Office of Personnel Management
DLA:	Defense Logistics Agency	OSD:	Office of the Secretary of Defense
DOD:	Department of Defense	OSTP:	Office of Science and Technology Policy
DOE:	Department of Energy	OVP:	Office of the Vice President
DOT:	Department of Transportation	PC:	Peace Corps
DSS:	Defense Security Service	PFIAB:	President's Foreign Intelligence Advisory Board
DTRA:	Defense Threat Reduction Agency	PIDB:	Public Interest Declassification Board
ED:	Department of Education	SBA:	Small Business Administration
EPA:	Environmental Protection Agency	SEC:	Securities and Exchange Commission
Ex-Im Bank:	Export-Import Bank of the United States	SSS:	Selective Service System
FBI:	Federal Bureau of Investigation	State:	Department of State
FCC:	Federal Communications Commission	Treasury:	Department of the Treasury
FEMA:	Federal Emergency Management Agency	TVA:	Tennessee Valley Authority
FMC:	Federal Maritime Commission	USAID:	United States Agency for International Development
FRS:	Federal Reserve System	USCENTCOM:	United States Central Command
GSA:	General Services Administration	USDA:	United States Department of Agriculture
HHS:	Department of Health and Human Services	USD(I):	Under Secretary of Defense for Intelligence
HSC:	Homeland Security Council	USEUCOM:	United States European Command
HUD:	Department of Housing and Urban Development	USITC:	United States International Trade Commission
Interior:	Department of the Interior	USJFCOM:	United States Joint Forces Command
ISCAP:	Interagency Security Classification Appeals Panel	USMC:	United States Marine Corps
ISOO:	Information Security Oversight Office	USNORTHCOM:	United States Northern Command
JCS:	Joint Chiefs of Staff	USPACOM:	United States Pacific Command
Justice:	Department of Justice	USPS:	United States Postal Service
Labor:	Department of Labor	USSOCOM:	United States Special Operations Command
MCC:	Millennium Challenge Corporation	USSOUTHCOM:	United States Southern Command
MDA:	Missile Defense Agency	USSTRATCOM:	United States Strategic Command
MMC:	Marine Mammal Commission	USTR:	Office of the United States Trade Representative
MSPB:	Merit Systems Protection Board	USTRANSCOM:	United States Transportation Command
NARA:	National Archives and Records Administration	VA:	Department of Veterans Affairs
NASA:	National Aeronautics and Space Administration		
Navy:	Department of the Navy		
NGA:	National Geospatial-Intelligence Agency		
NISP:	National Industrial Security Program		



INFORMATION SECURITY OVERSIGHT OFFICE

National Archives Building
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

Telephone: 202.357.5250
Fax: 202.357.5907
E-mail: isoo@nara.gov
Web site: www.archives.gov/isoo